

REMARKS

1. Applicant thanks the Examiner for his remarks and observations.

2. It should be appreciated that Applicant has elected to amend Claims 1 and 38 solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making such amendments, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

3. Claims 1 – 6, 8-16; 18 – 21 stand rejected under 35 USC 102(b) as being anticipated by U.S. Patent No. 5,166,866 ("Molnar"). Applicant respectfully disagrees.

A. There is no teaching in Molnar of a software package that includes "an access and control portion, said access and control portion affording selective access to any of said first and second objects." Molnar does teach "...execution may alternatively require the use of additional information that may be acquired either from the broadcast stream, from a remote site via the modem #40, or through entry of authorization information by the user ..." (Col. 16, line 36 to line 40); and Molnar also describes information being organized into "blocks", in broadcast memory, wherein each block includes a header to identify the block, the header operating to "convey validation information need to control access to the information in this or other blocks" (Col. 4, Line 44 to line 61). Molnar refers here, of course, to transmission units, such as packets (shown in Figures 2 and 3), wherein each transmission unit includes a header. However, there is no teaching of an access and control portion as a distinct component of a multi-object software package.

B. There is no teaching in Molnar of a software package that includes a notifier. While, Molnar does describe a header, as indicated above, one skilled in the art, based on Molnar's description at Col 4, line 50 to Col. 5, line 18 would understand the header in its usual sense as a data structure that precedes the main body of the transmission unit, containing information with which the transmission unit is identified. But there is no description of a notifier that is included as a component of a software package.

C. There is no teaching in Molnar of "installing said software package on said buyer's computer system." In fact Molnar specifically teaches that the preview software is not installed on the user's computer system, "...there are no hard copies of previewed programs (i.e. ...hard disk)" (Col 16, line 14 to line 16, emphasis added).

D. Regarding Claim 2: There is no teaching whatsoever in Molnar of an "access and control portion" that "includes usage authorization information" that is included in the software package.

E. Regarding Claims 4 and 5: While Molnar does teach storing the preview software on a hard disk at the transmitting unit (Col 4, line 4 to line 6, emphasis added), there is no teaching in Molnar of "saving said software package to a mass storage device in said user's computer" or "wherein said mass storage device comprises a hard disk drive."

F. Regarding Claim 6: There is no teaching in Molnar of "wherein said first object and said usage authorization information are encrypted." Molnar teaches that the program offered for review "may alternatively offer restricted subsets of the features of purchasable version, or their execution may alternatively require the use of additional information..." (Col 16, line 34 to line 37). Thus, access to the software may be restricted, but there is no teaching that any portion of it is encrypted. The header may also operate to "convey encryption information" (Col 4, line 58 to line 59, emphasis added). Thus, the whole transmission signal itself may be encrypted. But Molnar doesn't describe encryption of usage authorization information.

G. Regarding Claim 8: There is no teaching in Molnar of usage authorization information that "specifies any of:

permitted uses for said software product and individual components thereof and prices for said permitted uses;

authorized extent of use, where said extent of use comprises any of duration of use and number of uses, and prices for said authorized extent of use;

5 content of levels, where said software is purchased in succeeding levels and prices for said levels;

an authorized user for said software product subsequent to purchase; and

subsequent to purchase, which of said individual components and levels have been purchased, and which are still available for purchase." Applicant is unable to find
10 any part of the drawings and specification in Molnar that remotely teach or suggest the above.

H. Regarding Claim 12: Molnar is overwhelmingly directed to a "System to Demonstrate and Sell Computer Programs" (title). There is no teaching in Molnar of
15 "said data objects comprise any of digital images, video data objects and audio data objects." Col. 3, line 41 of Molnar merely describes what the carrier wave might be. There is no teaching of a software package that includes video data objects.

I. Regarding Claim 16: As above, there is no teaching in Molnar of a notifier,
20 particularly not a notifier that includes an "executable code section; and information required by said user for purchasing rights to said software product and enabling entry of transaction information required for said purchase of said rights." While Col. 15 of Molnar describes the process of purchasing software, not a single step of the process involves a notifier that is a component of the software package itself.

25 J. Regarding Claims 18 – 21, as above, Molnar describes a purchase process, but it is not accomplished through a notifier that it itself a part of the software package, furthermore Molnar does not teach:

30 "selecting one or more use options from a listing of said use options available, said available options being those objects available free of charge or those previously

purchased by said user, said listing being provided by said executable code section
accessing said usage authorization information, and wherein one or more of said
available objects are retrieved by said executable code section and loaded into
memory; and

5 executing said requested use.”

Accordingly the rejection of Claim 1 under 35 USC § 102(b) and all Claims depending
therefrom as being anticipated by Molnar is deemed to be improper.

10 4. Claims 1, 2, 6, 8 – 11, 13 – 16, 18 and 19 stand rejected under 35 USC § 102(b)
as being anticipated by U.S. Patent No. 5,224,166 (“Hartman”). Applicant respectfully
disagrees.

A. Although not entirely clear, the Examiner apparently relies on Col. 1, line 5 – 11
15 of Hartman as teaching:

“acquiring a software package, said software package comprising:

a first object, said first object a full-featured version of at least one
software product, wherein said user is denied access to said first object;

a second object, said second object a further version of said software
20 product having some, but less than all, of the features of said first object.”

The cited teaching merely describes the field of Hartmann’s invention “a system for
seamlessly processing encrypted and non-encrypted data and instructions, and more
particularly, to a data processing system that incorporates cryptographic architectural
25 features that inhibit unauthorized usage of encrypted media.” Hartmann thus describes
a processing unit that is capable of processing both encrypted and non-encrypted data

and instructions. "Seamlessly" presumably means that the user is unaware when the data and instructions processed are encrypted and when they are non-encrypted. The entire specification is devoted to a description of the processing unit, and the manner in which it process data and instructions. Virtually nothing is said about the media, nor is anything said about the ultimate use to which Hartmann's processing unit is to be put.

5 There is thus no teaching or suggestion of a software package as described in Claim 1. The Examiner is directed to Figure 1 of Hartmann. The media provider 10, encrypts (clear) media 17 to produce (encrypted) media 22, which is somehow delivered to remote processor 18. (Encrypted) media 22 is again shown in Figure 2. Beyond that,

10 there is no description of the media, 17 or 22 that would lead one skilled in the art to conclude that the software package of the Claimed invention was being described.

Referring now to Figure 2 of Hartmann, each segment register 56 includes a field 60 that indicates whether the data held in a particular register is encrypted or non-

15 encrypted. The reference is completely silent as to where the non-encrypted data comes from. Furthermore, the Claimed invention has nothing to do with seamless processing of encrypted and non-encrypted data. The Claimed invention relates to the evaluation of software for purchase, wherein the evaluation software is provided as a package, the package containing separate objects comprising an evaluation copy

20 having a reduced feature set, and the full-featured version, wherein user access to the full-featured version is denied.

Furthermore, there is no teaching or suggestion in Hartmann of "an access and control portion, said access and control portion affording selective access to any of said first and second objects." There is no teaching in Hartmann of first and second objects, or selective access to the objects. The Examiner is reminded that Hartmann provides seamless processing of encrypted and non-encrypted data. There is no access and control portion. The media provider 10 encrypts media 17, transmits it to the processor 18, and transmits media master keys to processor 18 after receiving processor 18's

25 30 public key (Figures 1 and 2). Where is the access and control portion of the software package?

There is further no teaching in Hartmann of a notifier. As described above, Hartmann's "software package" includes only the encrypted media.

35

There is no teaching in Hartmann of "installing said software package on said buyer's computer system." While Hartman describes in detail how the encrypted media 22 is processed once it is received at processor 18 (Cols. 6 and 7) there is no mention of permanently storing the media or installing it at the processor 18 in any way.

5

There is no teaching in Hartmann of accessing said second object, access to said second object being unrestricted. Because Hartmann doesn't teach first and second objects, it is impossible to teach a step of separately accessing a second object without accessing the first object. Furthermore, as previously pointed out, Hartmann is concerned with seamlessly processing encrypted and non-encrypted data and instructions.

10

There is further no teaching in Hartmann of "evaluating said second object whereby said user assesses whether said software product meets said user's requirements." No user is ever mentioned in Hartmann, nor is there any indication of what use the decrypted data and instructions will be put to.

15

B. Regarding Claim 2: There is no teaching in Hartmann of "wherein said access and control portion includes usage authorization information." As above, Hartmann doesn't provide an access and control portion or usage authorization information.

20

C. Regarding Claim 6: There is no teaching or suggestion in Hartmann of "wherein said first object and said usage authorization information are encrypted, whereby said user is prevented from accessing and using said first object and said usage authorization information until said prospective user executes a purchase request, thereby acquiring a license to at least some of the rights to said software product." As previously discussed, there are no first and second objects in Hartmann, nor is usage authorization information provided as part of the package. There is no suggestion of a user executing a purchase request. The only thing remotely resembling a purchase request is the step of the processor 18 sending the public key 12, whereupon the media provider 10 furnishes the media master keys and media identifiers 16. However, Hartmann is merely describes an encryption scheme, it has nothing to do with distribution of software for evaluation by a prospective buyer.

25

30

D. Regarding Claims 8 – 11. The Examiner's line of reasoning in finding Claims 8 – 11 anticipated by Hartmann is completely unclear to Applicant. Hartmann neither teaches nor suggests usage authorization information that "specifies any of:

permitted uses for said software product and individual components thereof and

5 prices for said permitted uses;

authorized extent of use, where said extent of use comprises any of duration of use and number of uses, and prices for said authorized extent of use;

content of levels, where said software is purchased in succeeding levels, and prices for said levels;

10 an authorized user for said software product subsequent to purchase; and

subsequent to purchase, which of said individual components and levels have been purchased, and which are still available for purchase."

15 The only feature of Hartmann that remotely resembles the above are the media Identifiers 16 that "identify the encrypted media" (Col 4, line 22 to line 23.) But nothing beyond this is said about them.

20 E. Regarding Claims 13 – 16: Claims 13 – 16 describe the usage authorization information of Claims 9 and 11 in greater detail. As above, Hartmann doesn't even remotely suggest usage authorization information as taught by the invention.

F. Regarding Claim 18 and 19: As above, Hartmann does not teach or suggest an evaluating step, nor is there any suggestion of purchasing anything.

25 Therefore, the rejection of Claim and all Claims depending therefrom under 35 USC 102(b) as being anticipated by Hartmann is deemed to be improper.

5. Claims 17, 22 – 28 and 29 - 44 stand rejected under 35 USC 103(a) as being unpatentable over Molnar in view of U.S. Patent No. 5,598,470 ("Cooper"). Applicant
30 respectfully disagrees. In view of the above, the cited references, either separately or in

combination fail to teach all features of the Claimed invention. Accordingly, the rejection of Claims 17 and 22 - 28 under 35 USC 103(a) is deemed to be improper.

5 6. Claims 45 - 47 stand rejected under 35 USC 103(a) as being unpatentable over Molnar in view of U.S. Patent No. 6,006,328 ("Drake"). Applicant respectfully disagrees. In view of the above, the cited references, either separately or in combination, fail to teach all features of the Claimed invention. Accordingly, the rejection of Claims 45 - 47 under 35 USC 103(a) is deemed to be improper.

10 7. Claims 48 - 51 stand rejected under 35 USC 103(a) as being unpatentable over Molnar in view of Cooper and further in view of Grantz. Applicant respectfully disagrees. In view of the above, the cited references, either separately or in combination, fail to teach all features of the Claimed invention. Accordingly, the rejection of Claims 48 - 51 under 35 USC 103(a) is deemed to be improper.

15

CONCLUSION

In view of the above, the application is deemed to be in allowable condition. Therefore,
the Examiner is earnestly requested to withdraw all rejections and allow the application
5 to pass to issue as a U. S. Patent. Should the Examiner have any questions related to
the application, he is urged to contact applicant's attorney at the telephone number
given below.

10

Respectfully submitted,



Michael A. Glenn

Reg. No. 30,176

**RECEIVED
CENTRAL FAX CENTER**

OCT 22 2003

OFFICIAL

15

Customer No. 22862

#4/a
KWS
014/014

RECEIVED
CENTRAL FAX CENTER

OCT 22 2003

OFFICIAL

CLAIM AMENDMENTS

a' 1. (Currently amended) A method of evaluating software by a user for subsequent
5 purchase comprising the steps of:

acquiring a software package, said software package comprising:

a first object, said first object a full-featured version of at least one
software product, wherein said user is denied access to said first object;

10 a second object, said second object a further version of said software
product having some, but less than all, of the features of said first object;

an access and control portion, said access and control portion
affording selective access to any of said first and second objects; and
a notifier;

15 installing said software package on said buyer's computer system, ~~wherein said
installation comprises running a setup routine;~~

accessing said second object, access to said second object being unrestricted;
and

evaluating said second object whereby said user assesses whether said software
product meets said user's requirements.

20

2. (Original) The method of Claim 1, wherein said access and control portion
includes usage authorization information.

3. (Original) The method of Claim 1, wherein said acquiring step comprises any of the steps of:

acquiring said software package as a software copy on a recordable medium;

5 acquiring said software package via data communication from any of an Internet site and a dial-up online service.

4. (Original) The method of Claim 3, said acquiring step further comprising the step of saving said software package to a mass storage device in said user's computer.

10 5. (Original) The method of Claim 4, wherein said mass storage device comprises a hard disk drive.

6. (Original) The method of Claim 2, wherein said first object and said usage
15 authorization information are encrypted, whereby said user is prevented from accessing and using said first object and said usage authorization information until said prospective user executes a purchase request, thereby acquiring a license to at least some of the rights to said software product.

20 7. (Original) The method of Claim 6, wherein said first object, said second object and said usage authorization information are macro-compressed and optionally, micro-compressed.

8. (Original) The method of Claim 6, wherein said usage authorization information specifies any of:

permitted uses for said software product and individual components thereof and prices for said permitted uses;

5 authorized extent of use, where said extent of use comprises any of duration of use and number of uses, and prices for said authorized extent of use;

content of levels, where said software is purchased in succeeding levels, and prices for said levels;

an authorized user for said software product subsequent to purchase; and

10 subsequent to purchase, which of said individual components and levels have been purchased, and which are still available for purchase.

9. (Original) The method of Claim 8, wherein said software product comprises one or more executable objects.

15

10. (Original) The method of Claim 9, wherein said executable objects comprise any of application software, utilities, and computer games.

11. (Original) The method of Claim 8, wherein said software product comprises one or more data objects.

20

12. (Original) The method of Claim 11, wherein said data objects comprise any of digital images, video data objects and audio data objects.

13. (Original) The method of Claim 9 wherein said levels comprise versions of said executable objects having more features enabled than a version in a preceding increment.

5 14. (Original) The method of Claim 9, wherein said increments comprise additional objects over those in a preceding increment.

15. (Original) The method of Claim 11, wherein said increments comprise additional objects over those in a preceding increment.

10 16. (Original) The method of Claim 9, wherein said notifier comprises:
an executable code section; and
information required by said user for purchasing rights to said software product and enabling entry of transaction information required for said purchase of said rights.

15 17. (Currently amended) The method of Claim 16, wherein said installing step comprises the steps of:

loading said software package into the memory of said user's computer system;
running a setup routine, wherein said executable code section performs normal
20 setup functions, including displaying a user license; and
agreeing to terms of said user license.

18. (Original) The method of Claim 16, wherein said evaluating step comprises the steps of:

a' selecting one or more use options from a listing of said use options available, said available options being those objects available free of charge or those previously purchased by said user, said listing being provided by said executable code section accessing said usage authorization information, and wherein one or more of said
5 available objects are retrieved by said executable code section and loaded into memory; and
executing said requested use.

19. (Original) The method of Claim 18, further comprising the step of:

10 purchasing any of said software product in entirety and one or more parts thereof.

20. (Original) The method of Claim 19, wherein said purchasing step comprises the steps of:

15 providing user information;

optionally, electing usage levels and desired features;

providing payment information;

transmitting a purchase request to a server, said purchase request comprising said payment information and said desired usage information.

20

21. (Original) The method of Claim 20, wherein said payment information comprises credit card information and contact information for said prospective purchaser.

22. (Original) The method of Claim 21, wherein selected information characteristic of said user's computer system is transmitted to said server after said purchase request is received by said server

5 23. (Original) The method of Claim 22, wherein said selected information includes serial numbers from any of a hard disk drive, a network interface card, and a mother board from said user's computer.

24. (Original) The method of Claim 23, wherein said selected information includes an
10 identification code identifying a particular storage medium on which said software package was distributed.

25. (Original) The method of Claim 22, wherein said server transmits an access control code to said user's computer after said purchase request is successfully
15 processed, said access control code based on said selected information characteristic of said user's computer, and wherein said access control code is separately stored on said user's computer from said software package.

26. (Original) The method of Claim 25, wherein said access control code is a
20 decryption key for said encrypted first object, said decryption key based on said selected information, and wherein both said decryption key and said selected information must be present on said user's computer in order to decrypt said first object.

27. (Original) The method of Claim 26, wherein said decryption key is split into two parts, a first part of which is calculated on said server, and a second part of which is calculated in real time on said user's computer using said selected information.

5 28. (Original) The method of Claim 25, wherein said access control code is a decryption executable for said encrypted first object, said decryption executable based on said selected information, and wherein both said decryption executable and said selected information must be present on said user's computer in order to decrypt said first software version.

10

29. (Original) The method of Claim 11, wherein said access control portion further comprises a signature, said signature being readable by a predetermined executable serving to control access to said first object.

15 30. (Original) The method of Claim 29, wherein said predetermined executable is a driver executable, wherein said driver executable is downloaded from a server by said user; and

wherein said driver executable is installed on said user's computer separately from said software package.

20

31. (Original) The method of Claim 30, wherein said notifier comprises means for notifying said prospective user to download said driver executable from said server.

32. (Original) The method of Claim 31, wherein said driver executable reads said signature and recognizes said software package as one containing data objects, wherein said software package requires access control by said driver executable.

5 33. (Original) The method of Claim 32, wherein said driver executable decrypts said usage authorization information, whereby said usage authorization is presented to said user.

Q1

10 34. (Original) The method of Claim 33, wherein said evaluating step further comprises the steps of;

selecting one or more use options from a listing of said use options available, said available options being those objects available free of charge or those previously purchased by said user, said listing being provided by said driver executable accessing said usage authorization information, and wherein one or more of said available objects
15 are retrieved by said driver executable and loaded into memory; and
executing said requested use.

35. (Original) The method of Claim 34, further comprising the step of:
purchasing any of:
20 said software product in entirety; and
one or more parts thereof.

36. (Original) The method of Claim 35, wherein said purchasing step comprises the steps of:

providing user information;

optionally, electing usage levels and desired features;

providing payment information;

transmitting a purchase request to a server, said purchase request comprising

5 said payment information and said desired usage information.

37. (Original) The method of Claim 36, wherein said payment information comprises credit card information and contact information for said prospective purchaser.

10 38. (Currently amended) The method of Claim 37, wherein selected information characteristic of said user's computer system is transmitted to said ~~said~~ server ~~receives~~ server after said purchase request.

39. (Original) The method of Claim 38, wherein said selected information includes
15 serial numbers from any of a hard disk drive, a network interface card, and a motherboard from said user's computer.

40. (Original) The method of Claim 39, wherein said selected information includes an
20 identification code which identifies a particular storage medium on which said software package was distributed.

41. (Original) The method of Claim 38, wherein said server transmits an access control code to said user's computer after said purchase request is successfully processed, said access control code based on said selected information characteristic

of said user's computer, and wherein said access control code is separately stored on said user's computer from said software package.

42. (Original) The method of Claim 41, wherein said access control code is a decryption key for said encrypted first object, said encryption key based on said selected information, and wherein both said decryption key and said selected information must be present on said user's computer in order to decrypt said first object.

43. (Original) The method of Claim 42 wherein said encryption key is split into two parts, a first part of which is calculated on said server, and a second part of which is calculated in real time on said user's computer using said selected information.

44. (Original) The method of Claim 43, wherein said access control code is a decryption executable for said encrypted first object, said encryption executable based on said selected information, and wherein both said decryption executable and said selected information must be present on said user's computer in order to decrypt said first software version.

45. (Original) The method of Claim 1, wherein said software package includes means for protecting said software package against class attacks and dump attacks.

46. (Original) The method of Claim 45, wherein said protection against dump attacks comprises any of erasing and modifying one or more of said objects' relocation

information, directory pointers, or entry point after said objects have been written into memory.

47. (Original) The method of Claim 45, wherein said protection against dump attacks
5 comprises modifying references to external routines in an import table of said objects
whereby said notifier controls access to said routines.

48. (Original) The method of Claim 25, wherein said server inserts transaction
information in said software product as a watermark.

10

49. (Original) The method of Claim 41, wherein said server inserts transaction
information in said software product as a watermark.

15

50. (Original) The method of Claim 25, wherein said server inserts transaction
information in said access control code as a watermark.

51. (Original) The method of Claim 41, wherein said server inserts transaction
information in said access control code as a watermark.

20